99

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/750,921	01/02/2001	Kyoung Jin Kang	P-170	7352

34610 7590 10/24/2005

FLESHNER & KIM, LLP
P.O. BOX 221200
CHANTILLY, VA 20153

EXAMINER	
CHAI, LONGBIT	
ART UNIT	**PAPER NUMBER**
2131	

DATE MAILED: 10/24/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/750,921	**Applicant(s)** KANG ET AL.	
	Examiner Longbit Chai	**Art Unit** 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on 12 September 2005.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) 1,5-18 and 20 is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) 1,5-18 and 20 is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on 05 April 2005 is/are: a)☒ accepted or b)□ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) □ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date _____.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

1. Claims 2 – 4 and 19 have been canceled; claims 1 and 6 have been amended in an amendment filed on 4/5/2005.

Continued Examination Under 37 CFR 1.114

2. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 3/4/2005 has been entered.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

3. Claim 1 is rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal et al. (PN: 5657390), in view of WAP Wireless Communication (hereinafter, "WWC" – WAP Wireless Communication Protocols Directory – WTLS/WTP/WSP), and in view of Ganesan (PN: 5535276).

As per claim 1, Elgamal teaches a security protocol structure in an application layer of a Wireless Application Protocol (WAP) standard, comprising:

Elgamal teaches a secure session layer directly between a session layer and an application layer (Elgamal: Column 12 Line 13 – 19 and Column 11 Line 14 – 18, Column 6 Line 10 – 17 and Column 5 Line 20 – 25: this particular secure session layer is considered as the sockets API (Application Program Interface) plus SSL library protocol, where the applications can setup a socket connection (Elgamal: Column 6 Line 10 – 13) and further allow the applications to call and encrypt / decrypt information passed through this established socket connection (Elgamal: Column 12 Line 13 – 15) because this socket connection is indeed the transport layer protocol that uses socket type connection (Elgamal: Column 12 Line 18 – 19), where TCP socket connection (or session link) indeed forms a session layer transport in the commonly known seven-layer ISO/OSI reference model as compared with the typical Internet protocol model where it lacks the session layer (Elgamal: Column 11 Line 14 – 18). Thereby, the secure session layer between the application layer and a transport layer (Elgamal: Column 6 Line 15 – 17) is indeed between the application layer and a session layer because transport layer protocol that uses socket type connection, as taught by Elgamal, is equivalent to the session layer in the ISO/OSI reference model as addressed above).

However, Elgamal does not disclose expressly, in the wireless application environment and protocols, a secure session layer directly between a session layer and an application layer.

WWC teaches, in the wireless application environment and protocols, a session layer including a wireless session protocol and an application layer including a wireless application environment (WWC: Page 6: WSP and WAP).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of WWC within the system of Elgamal because WWC teaches Wireless Application Protocol aims to provide Internet content and advanced telephony services to digital mobile phones, pagers and other wireless terminals across different wireless network environments and allow their users to respond to e-mail, access computer databases and to empower the phone to interact with Internet-based content and e-mail.

Accordingly, Elgamal in view of WWC does teach:

a secure session layer directly between a session layer including a wireless session protocol and an application layer including a wireless application environment.

a transaction layer including a wireless transaction protocol (WWC: Page 4) below the session layer;

a security layer including a wireless transport layer security (WWC: Page 3) below the transaction layer;

a transport layer including a wireless datagram protocol (WWC: Page 6) below the security layer;

a network layer below the transport layer (Elgamal: Figure 8),

wherein the secure session layer provides a data security function in the application layer, and includes a secured session layer security (SSLS) protocol to provide a secure session interface to an application program, and wherein secure communication is established between a server and a client using the SSLS protocol and without using a certificate or public/private key generation operation (Elgamal: Column 12 Line 13 – 19 and Column 11 Line 14 – 18, Column 6 Line 10 – 17 and Column 5 Line 20 – 25). However, Elgamal does not disclose expressly without using a certificate or public / private key generation operation.

Elgamal teaches using the client's certificate is optional (Elgamal: see for example, Column 21 Line 47).

Ganesan teaches using symmetric algorithms instead of using a certificate or public / private key generation operation (i.e. asymmetrical algorithms) (Ganesan: see for example, Column 1 Line 29 – 57).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Ganesan within the system of Elgamal as modified because (a) Elgamal teaches the disclosure references public key algorithms in general; but, it will be appreciated that the discussions can be applied to different security mechanisms (Elgamal: see for example, Column 6 Line 46 – 51) and (b) Ganesan teaches the symmetric algorithm can be another security alternative to asymmetric algorithm because it is fairly efficient and can be used for fairly high data rates, especially when appropriate hardware implementations are used (Ganesan: see for example, Column 1 Line 29 – 57 and Column 1 Line 44 – 46).

4. Claims 5, 6, 8, 10 – 15 and 18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal et al. (PN: 5657390), in view of WAP Wireless Communication (hereinafter, "WWC" – WAP Wireless Communication Protocols Directory – WTLS/WTP/WSP), in view of Ganesan (PN: 5535276), and in view of Chen et al. (PN: US 6182220 B1).

As per claim 5, Elgamal as modified does not teach a shared secret value is stored by a client and a server, and wherein the shared secret value is a pre-master secret.

Chen teaches a shared secret value is stored by a client and a server, and wherein the shared secret value is a pre-master secret (Chen: see for example, Column 3 Line 48 – 52: Chen teaches the authentication mechanism for encryption and decryption includes the parameter of a user variable name (or a plain text password) in addition to the client random and server random values. The parameter of a user variable name (or a plain text password) is qualified as a shared pre-master secret value stored by a client and a server).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen within the system of Elgamal as modified because Chen teaches (a) an improved system and method for building encrypted information (Chen: see for example, Column 1 Line 55 – 58), and (b) an enhanced client can generate a compatible encrypted secret using the proposed parameters and block cipher techniques between the client and server without using asymmetric public/private key (Chen: see for example, Column 3 Line 44 – 46) to deliver the client master secret so that the user cost can be reduced especially in the low bandwidth wireless environment.

As per claim 6, the claim limitations are met as the same reasons as that set forth in the paragraph above regarding to claim 1 with the exception of the following feature receiving a first message containing a client random value from a client; determining whether the first message is a valid message; extracting a pre-master secret from the first message; generating a specific server random value; generating and transmitting a second message to the client to pass the server random value to the client; generating a master secret in accordance with the extracted pre-master secret, client random value, and server random value; generating a key block in accordance with the master secret, client random value, and server random value; generating from the key block an encryption key value for encryption and decryption algorithms and Message Authentication Code (MAC) algorithms; generating a third message indicating that encryption is activated; and generating a fourth message to verify that the client has generated a client master secret identical to the master secret.

However, Elgamal teaches receiving a first message containing a client random value from a client (Elgamal: see for example, Column 22 Line 1 – 4);

determining whether the first message is a valid message (Elgamal: see for example, Column 22 Line 3 – 4);

Elgamal does not teach extracting a pre-master secret from the first message.

Chen teaches extracting a pre-master secret from the first message (Chen: see for example, Column 3 Line 41 – 52: Chen discloses the server extracts the plain text password based on the client ID (or user name) in order to generate a encrypted secret (i.e. encrypted password) compatible to the one that the client creates. The plain text password is qualified as a pre-master secret between the client and the server);

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Chen within the system of Elgamal because Chen teaches (a) an improved system and method for building encrypted information (Chen: see for example, Column 1 Line 55 – 58), and (b) an enhanced client can generate a compatible encrypted secret using the proposed parameters and block cipher techniques between the client and server without the need using asymmetric public/private keys (Chen: see for example, Column 3 Line 44 – 46) to deliver the client master secret so that the user cost can be reduced especially in the low bandwidth wireless environment.

generating a specific server random value (Elgamal: see for example, Figure 4 and Column 23 Line 27 – 28);

generating and transmitting a second message to the client to pass the server random value to the client (Elgamal: see for example, Figure 4);

Elgamal does not teach generating a master secret in accordance with the extracted pre-master secret, client random value, and server random value.

generating a master secret in accordance with the extracted pre-master secret, client random value, and server random value (Chen: see for example, Column 3 Line 48 – 51);

generating a key block in accordance with the master secret, client random value, and server random value (Elgamal: see for example, Column 22 Line 3 – 4: Elgamal teaches that CHALLENGE reads on client random and CONNECTION-ID reads on server random as CONNECTION-ID is a string of randomly generated bytes (Elgamal: see for example, Column 23 Line 27 – 28);

generating from the key block an encryption key value for encryption and decryption algorithms and Message Authentication Code (MAC) algorithms (Elgamal: see for example, Column 28 Line 37 – 49: Elgamal teaches session key production phase where MAC key and the encryption /decryption keys for the client and server is obtained from the key block);

generating a third message indicating that encryption is activated (Elgamal: see for example, Figure 5 and Column 28 Line 51: Elgamal teaches the first message is client-hello message, the second message (from the server) is server-hello message, the third message (from the client) is the client-finish message (or client ChangeCipherSpec message), the fourth message (from the server) is server-verify message which indicates all the message data is encrypted (i.e. encryption is activated) and indicate the client is ready to verify the encrypted information from the server and the very last message (from the server) is server-finish message that include the entire encrypted handshake record being sent by the server to be verified by the client).

generating a fourth message to verify that the client has generated a client master secret identical to the master secret and to indicate that secured communication has been established between a server generating the server random value and the client (Elgamal: see for example, Figure 5 and Column 32 Line 7 – 37: It would have been obvious to a person of ordinary skill in the art to understand switching the message sequence between the server-finish and client-finish messages to accommodate the server ChangeCipherSpec message as the third message and the client-finish (or client ChangeCipherSpec) message as the very last message to complete the message handshake process because (a) Elgamal as modified teaches that the client has no need to send the master key to the server and, instead, the master key is generated from the pre-master secret pre-stored at the client and server sides and thereby there is no need for the client to activate ChangeCipherSpec (or client-finish) message in advance to the server finish message after the master key has been sent during the regular SSL protocol section, and (b) either way would work just equally efficient);

As per claim 8, Elgamal as modified further teaches the pre-master secret is a shared pre-master secret, and wherein the server manages the shared pre-master secret corresponding to the first message in a database (Chen: see for example, Column 3 Line 48 – 52: Chen teaches the authentication mechanism for encryption and decryption includes the parameter of a user variable name (or a plain text password) in addition to the client random and server random values. The parameter of a user variable name (or a plain text password) is qualified as a shared pre-master secret value managed by the server corresponding to the index of userID sent in the first client-hello message).

As per claim 10, Elgamal as modified further teaches the fourth message is a Finished message, and is transmitted from a record layer (Elgamal: see for example, Figure 5 and Column 30 Line 56 and Column 32 Line 10 – 13).

As per claim 11, Elgamal as modified further teaches the Finished message is transmitted using the encryption key and MAC key values, and indicates that encrypted communications have been established (Elgamal: see for example, Column 30 Line 56 – 57, Column 32 Line 15 – 18 and Column 32 Line 29 – 30).

As per claim 12, Elgamal as modified teaches the claimed invention as described above (see claim 6). Elgamal as modified further teaches the client computes values of the master secret, the key block, the encryption key, and the MAC key after receiving and processing the second message (see same rationale addressed above in rejecting claim 6).

As per claim 13, Elgamal as modified further teaches the third message is a ChangeCipherSpec message (see same rationale addressed above in rejecting claim 6).

As per claim 14, Elgamal as modified further teaches the encryption key is extracted from the key block in such a manner that a 16 byte client MAC key, 16 byte client encryption key, 8 byte client IV, 16 byte server MAC key, 16 byte server encryption key, and 8 byte server IV are sequentially allocated from the key block (Elgamal: see for example, Column 26 Line 40 – 50 and Column 25 Line 31 – 34).

As per claim 15, Elgamal as modified further teaches the first message and the second message comprise a Handshake message (Elgamal: see for example, Figure 5).

As per claim 18, Elgamal as modified further teaches the client verifies that encryption is activated after receiving and processing the third message (see same rationale addressed above in rejecting claim 6).

5. Claims 7, 9 and 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal et al. (PN: 5657390), in view of WAP Wireless Communication (hereinafter, "WWC" – WAP Wireless Communication Protocols Directory –

WTLS/WTP/WSP), in view of Ganesan (PN: 5535276), in view of Chen (PN: US 6182220), and in view of Wall et al. (PN: 6654806).

As per claim 7, Elgamal as modified does not teach the client random value is a client ID.

Wall teaches the client random value is a client ID (Wall: see for example, Column 10 Line 63 – 67 and Column 11 Line 1 – 4: Wall teaches 64-bit number UserID and 128-bit random number secret code entered on a client terminal by a subscriber from the smart card – This user information stored on the smart card is qualified to be used as the unique identifier for the client).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Wall within the system of Elgamal as modified because Wall discloses the interconnect fabric implemented in a wireless environment using smart card (Wall: see for example, Column 8 Line 63 – 65).

As per claim 9, Elgamal as modified does not teach the client random in the first message is a client ID entered on a client terminal by a subscriber.

Wall teaches the first message is a client ID entered on a client terminal by a subscriber from the smart card (Wall: see for example, Column 10 Line 63 – 67 and Column 11 Line 1 – 4: Wall teaches the client ID carries a random number. Therefore, it would have been obvious to a person of ordinary skill in the art at the time the invention was made to modify that the first message random value comes from the client ID because Wall teaches the client ID carries a random number). Same rationale of combination applies here as above in rejecting the claim 7.

As per claim 20, Elgamal as modified does not teach a subscriber inputs the client ID into a wireless communications device to establish secure communications with a server using the Wireless Application Protocol.

Wall teaches a subscriber inputs the client ID into a wireless communications device through the smart card (Wall: see for example, Column 8 Line 63 – 65, Column 10 Line 63 – 67 and Column 11 Line 1 – 4). Same rationale of combination applies here as above in rejecting the claim 7.

6. Claims 16 and 17 are rejected under 35 U.S.C. 103(a) as being unpatentable over Elgamal et al. (PN: 5657390), in view of WAP Wireless Communication (hereinafter, "WWC" – WAP Wireless Communication Protocols Directory – WTLS/WTP/WSP), in view of Ganesan (PN: 5535276), in view of Chen et al. (PN: US 6182220), and in view of Binding et al. (PN: 6694431).

As per claim 16, Elgamal as modified does not teach the Handshake message is formed by concatenating the first message and the second message.

Binding teaches the Handshake message is formed by concatenating the first message and the second message (Binding: see for example, Column 4 Line 51 – 55).

It would have been obvious to a person of ordinary skill in the art at the time the invention was made to combine the teaching of Binding within the system of Elgamal as modified because Binding teaches a message piggy-backed technique for establishing and maintaining end-to-end security session while providing a secure low-overhead connection between a client and server application (Binding: see for example, Column 4 Line 4 Line 47 – 49).

As per claim 17, Elgamal as modified further teaches the second message is a ServerHello message, the third message is a ChangeCipherSpec message, and the fourth message is a Finished message (see same rationale addressed above in rejecting claim 6).

Elgamal as modified does not teach the second, third, and fourth messages are concatenated together to be transmitted to the client.

Binding teaches the second, third, and fourth messages are concatenated together to be transmitted to the client (Binding: see for example, Column 4 Line 4 Line 51 – 65). Same rationale of combination applies here as above in rejecting the claim 16.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Longbit Chai whose telephone number is 571-272-3788. The examiner can normally be reached on Monday-Friday 8:00am-4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on 571-272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Longbit Chai
Examiner
Art Unit 2131

LBC
LBC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100